BEFORE THE

Federal Communications Commission

WASHINGTON, D.C.

In the matter of	)	
	)	
Amendment of Parts 0, 1, 2, 15, and 18 of the Commission's Rules Regarding Authorization of Radiofrequency Equipment	)	ET Docket No. 15-170
	)	
Request for the Allowance of Optional Electronic Labeling for Wireless Devices	)	RM-11673

COMMENTS OF LAURENCE BRETT ("BRETT") GLASS, d/b/a LARIAT, A WIRELESS INTERNET SERVICE PROVIDER SERVING ALBANY COUNTY, WYOMING

Laurence Brett ("Brett") Glass, a sole proprietor doing business as LARIAT, a wireless Internet service provider serving Albany County, Wyoming, pursuant to Section 1.415 of the Commission's Rules (47 C.F.R. §1.415), hereby respectfully submits the following comments in response to the *Notice of Proposed Rule Making*, FCC 15-92, released July 21, 2015 (the Notice)[1], which proposes to modify the Commission's rules regarding the evaluation, approval, marketing, and labeling of RF devices.

LARIAT was the first of the many wireless Internet service providers (WISPs) now doing business within the continental United States. LARIAT provides high quality, high speed broadband Internet service to a large service area in rural Wyoming. LARIAT was originally founded as a nonprofit, 501(c)(12) rural telecommunications cooperative, and was taken private by its founder, Laurence Brett ("Brett") Glass, at the request of the membership in 2003. An electrical engineer with an MSEE from

[1]Amendment of Parts 0, 1, 2, 15 and 18 of the Commission's Rules Regarding Authorization of Radiofrequency Equipment, *Notice of Proposed Rulemaking*, 30 FCC Rcd 7725 (2015).

Stanford University, Brett was present at the University during the TCP/IP transition and helped to modify computer hardware, software, and operating systems to interoperate with the ARPAnet and NSFNet, which in turn evolved into what is now the Internet. While at Stanford, he also participated in the development of digital radios designed to operate on unlicensed frequencies – work which was incorporated into the ancestors of today's Wi-Fi equipment.

When the Internet involved from a research project to a network available to individual computers by dialup to the vast network of always-on networks it is today, consumers and business users found that they needed high quality Internet routers to make good and safe use of it. LARIAT, from its earliest days, has built, programmed, and maintained high performance, secure, reliable routers for itself and its customers. LARIAT has also been active in the realm of cybersecurity, finding and blocking Internet worms and malware so as to protect its networks, its customers and the Internet community at large.

While some of the rule changes proposed in the Notice are worthy of adoption or are even long overdue, others would prevent LARIAT and other Internet service providers from engaging in software modifications which lower the cost of Internet equipment to end users (encouraging adoption), improve performance, enhance security (engendering trust in the medium), and/or lower the cost of network deployment and maintenance. These changes would therefore violate the express directive from Congress, at 47 USC §1302 (commonly referred to as "Section 706"), which states:

> "The Commission and each State commission with regulatory jurisdiction over telecommunications services shall encourage the deployment on a reasonable and timely basis of advanced telecommunications capability to all Americans (including, in particular, elementary and secondary schools and classrooms) by utilizing, in a manner consistent with the public interest, convenience, and necessity, price cap regulation, regulatory forbearance, measures that promote competition in the local telecommunications market, or other regulating methods that remove barriers to infrastructure investment."[2]

These proposed changes would thus be not only undesirable but unlawful and therefore should not be adopted.

---

[2] 47 USC §1302(a)

In addition, the NPRM misses an opportunity to serve members of public by better informing them of the emissions characteristics of the equipment they own. LARIAT frequently has to address complaints from consumers which are caused by interference between users' own wireless equipment, or between their home or office wireless equipment and outdoor equipment used for the delivery of wireless broadband. Many of these incidents result from inadequate documentation: nowhere in the Commission's current rules is it required that equipment come with information stating what radio frequencies it uses, making it impossible for the layman to avoid interference between, for example, a Wi-Fi router and a pair of wireless headphones. While the proposed changes appropriately relax some labeling requirements for wireless equipment, it is imperative – as more and more devices go wireless – that the Commission insist that equipment be clearly marked as to the frequencies at which it may radiate so as to prevent such problems.

I. Custom firmware encourages adoption, lowers costs, reduces e-waste

Many of LARIAT's users require specialized network equipment. For example, a customer with a sprawling house, ranch, or workplace may need a device which simultaneously serves as a Wi-Fi access point and repeater, a 5-port Ethernet switch, and a VPN endpoint. Such a device can cost hundreds of dollars if purchased new – or, depending upon the combination of features required, may not be available at all. However, LARIAT can take an older or obsolete router – one which would otherwise be discarded and pollute the environment – and add custom firmware, such as OpenWRT, Tomato, or DD-WRT, to create a device that suits the user's needs for as little as $30 or $40. The result: a satisfied user, toxic metals and non-recyclable plastics spared from the landfill, and increased Internet adoption. LARIAT also uses routers incorporating customized operating system software internal to its own networks and to provide shared Internet access in apartment buildings and public venues such as coffeehouses and retail stores.

II. Custom firmware enhances cybersecurity

In early 2014, LARIAT began to receive calls from customers complaining of slow or erratic

Internet service. (Such problems are virtually always blamed on the ISP, regardless of their actual cause.) Monitoring of the packets flowing through users' connections – with their permission – revealed that something on their networks was scanning multiple subnets throughout the Internet, address by address, apparently looking for devices of a particular type. When the probes continued after all devices had been disconnected from the users' routers, we realized that the routers themselves were infected. This led to LARIAT's discovery of the Internet worm which SANS dubbed "TheMoon". [3] Nearly all current models of Linksys routers – the most popular brand in the world – were susceptible, including those operating on the 5 GHz band. The routers could be commandeered to make all sorts of mischief – spying on users, hijacking their connections, forming "botnet" armies to be used in denial of service attacks. Worse still, because Linksys had just been purchased by Belkin from Cisco and was undergoing the upheavals that typically follow a change in ownership, patched firmware was slow in coming – taking six months or longer, depending upon the model, to be released. LARIAT therefore closed the security hole by installing DD-WRT, a third party operating system, on users' routers.

Most of the Linksys routers affected by "TheMoon" were at least still for sale and therefore supported. Bu in other cases, perfectly good equipment which has been "orphaned" by the manufacturer – for reasons having nothing to do with its fitness for use – can only be made secure via third party firmware. For example, Ubiquiti has dubbed its Bullet 2 and Bullet 2HP Internet radios – used by millions of WISP customers – "legacy" products which will no longer be supported. Unfortunately, these radios have multiple security vulnerabilities, including limited password length and an administrative Web interface which uses the deprecated, insecure SSL3 protocol. Only by upgrading the radios to alternative firmware such as DD-WRT can these perfectly good devices – which would cost consumers in excess of $100 in parts and labor to replace – be secured while remaining in use.

---

[3] See https://isc.sans.edu/diary/Linksys+Worm+%22TheMoon%22+Summary%3A+What+we+know+so+far/17633

III. Banning custom firmware will not stop truly malicious parties

Ironically, while banning customized router firmware will preclude consumers, businesses, and ISPs with good intentions from doing innovative and productive things with their routers and radiofrequency equipment, it is unlikely to stop truly malicious parties that wish to violate FCC regulations and/or use spectrum which they are not permitted to use. Such parties will simply "jailbreak" the equipment – by hacking the hardware and/or finding vulnerabilities in the software – and do as they wish. Thus, the proposed rules will punish the innocent and frustrate legitimate attempts to innovate while doing nothing to deter the guilty.

IV. Proposed labeling rules should require clear disclosure of emitted frequencies

Finally, the proposed rules fail to require an important and long needed disclosure that would benefit consumers: the frequency or frequencies on which Part 15 equipment operates. LARIAT, as a wireless ISP, is frequently called upon to resolve network performance issues that result not from any flaw in its service but rather from RF interference between devices within the customer's home or business. The consumers experiencing the problems are unable to resolve them themselves, because they often cannot tell which frequencies, or even which frequency bands, their own equipment uses.

It thus behooves the Commission – again, as per its statutory obligation under Section 706 – to require that consumer RF equipment be clearly marked with the frequencies and/or frequency bands upon which it operates. It is preferable that this information be clearly marked on the equipment housing, if at all possible, so that consumers who lack knowledge of how to access an electronic "label" can nonetheless be informed as to the nature of its emissions.

V. Conclusion

As mentioned at the outset, many of the rule changes mentioned in the NPRM are desirable or even long overdue. However, any restriction which prevents the installation or customization of radio

firmware will deter innovation, threaten cybersecurity, present barriers both economic and logistical to broadband adoption, and fail to prevent interference with TDWR and other critical systems by malicious parties. Furthermore, the Commission should take this opportunity to inform consumers of possible interference between devices by modifying its labeling requirements to require disclosure of the frequencies upon which equipment operates.

Respectfully submitted,

/s/

Laurence Brett ("Brett") Glass, d/b/a LARIAT
PO Box 383
Laramie, WY 82073-0383